Commander, U. S. Fleet Forces Command
and
Commander, Marine Forces Command
Base, Station and Installation
Physical Security Assessment Report

September 27, 2013

Executive Summary

This report provides a "quick look" world-wide assessment of current physical security and access control measures at Navy and Marine Corps owned and operated installations, as directed by the Chief of Naval Operations and Commandant of the Marine Corps in a joint letter dated September 23, 2013. This assessment addresses adequacy of Navy and Marine Corps physical security directives and policies, as well as bases, stations and installation compliance with governing physical security and access control regulations and policies. A more in-depth physical security review will be completed no later than October 31, 2013--this second assessment will determine whether current procedures are appropriate and adequate and will recommend enhancements, improvements and innovations to be taken in the future. Both this "quick look" assessment and the more in-depth review are separate from the ongoing Washington Navy Yard investigation.

Assessment

U.S. Fleet Forces and U.S. Marine Forces Command examined current directives and policies governing physical security and access control for adequacy and compliance. This assessment identified the following:

- Existing physical security guidance and directives are detailed, valid and adequate.
- The Navy and Marine Corps are aligned with Department of Defense, Department of the Navy, and Service specific physical security guidance and directives.
- Navy and Marine Corps security forces are adequately trained and exercised to execute directed physical security guidance for appropriate force protection conditions based upon assessed risk.
- The Navy is in compliance with physical security protection standards set by Department of Defense, Department of the Navy, Service and Geographic Combatant Commander guidance and directives.
  - ➢ Navy installation physical security programs possess adequate response force capability either via organic security forces, as augmented by Auxiliary Security Forces, or through comprehensive Mutual Support Agreements with local, state and federal agencies; and Status of Forces Agreements with host nations.
- The Marine Corps is generally compliant with physical security protection standards set by Department of Defense, Department of the Navy, Service and Geographic Combatant Commander guidance and directives given risk mitigation measures in place.
  - ➢ The Marine Corps physical security and access control framework and supporting processes protect the force, systematically assess and manage risk, synchronize protection related programs/activities and prioritize investments. The ability to fully comply with physical security and access control standards is also influenced by the geophysical character of each

installation. Marine Corps installations rely on coordinated efforts with tenant commands and activities in support of mission assurance.

In a manner consistent with Service directives and policies, this "quick look" revealed that physical security is unique to each Service. The Navy and Marine Corps each operate with specific imperatives to maintain physical security and access control. Enclosures (1) and (2) provide additional information on these approaches and processes.

WILLIAM E. GORTNEY

R. T. Tryon
RICHARD T. TRYON

Navy Base, Station and Installation Physical Security Assessment Report

September 27, 2013

Encl (1)

Table of Contents

1. Tasking

Per tasking to Commander, U.S. Fleet Forces, contained in the joint Chief of Naval Operations/Commandant of the Marine Corps letter, "Base, Station, and Installation Physical Security Assessment," September 23, 2013: "Provide a 'quick look' assessment into current physical security and access control measures at U.S. Navy and Marine Corps owned and operated installations world-wide. Your assessment should address, but not be limited to, adequacy of Navy and Marine Corps security directives, as well as compliance with all directives and policies governing physical security and access control. Identify discrepancies across our bases, stations, and installations in their ability to comply with these directives and policies. This assessment is separate from the investigation of the Washington Navy Yard incident. This assessment shall be completed and forwarded no later than 27 September 2013. Conduct a second, more thorough physical security review that determines whether current procedures are appropriate and adequate and what additional enhancements, improvement and innovations might need to be taken in the future. This second assessment shall be completed and forwarded no later than 31 October 2013."

Tasks conducted in this assessment:

a. Specified tasks:
   i. Assess current physical security requirements at Navy owned and operated installations world-wide.
   ii. Assess access control to Navy owned and operated installations world-wide.
   iii. Determine adequacy of security directives.
   iv. Determine compliance with all directives and policies governing physical security and access control.

b. Implied tasks:
   i. Determine underlying assumptions with respect to physical security and installation access.
   ii. Determine adequacy of physical security and access control policy and guidance.
   iii. Assess forces' compliance to security policy and guidance.
   iv. Assess risk to forces world-wide.
   v. Assess the adequacy of force protection and security training to enable the setting of an appropriate force protection posture based upon risk.
   vi. Assess installation execution of physical security and access control policies at the tactical level.

Tasks that will be conducted in the second assessment:

a. Specified tasks:
   i. Conduct a second, more thorough physical security review that determines whether current procedures are appropriate and adequate.
   ii. Determine what additional enhancements, improvement and innovations might need to be taken in the future.

b. Implied tasks:
   i. Assess the adequacy of current physical security doctrine to mitigate postulated threats.
   ii. Identify barriers to physical security and access control policy implementation.
   iii. Recommend new or innovative procedures or policies that could improve our ability to provide security at our installations.

2. Physical Security and Access Control Policy and Guidance Directives

a. Presidential and Department of Defense policy and guidance directives:
   i. Presidential memorandum: "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs"
   ii. Homeland Security Presidential Directive (HSPD) 12, "Policies for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004
   iii. Secretary of Defense Directive-Type Memorandum (DTM) 09-012, "Interim Policy Guidance for DoD Physical Access Control," December 8, 2009
   iv. Deputy Secretary of Defense Memorandum, "Antiterrorism Building Standards for Leased Space," December 7, 2012
   v. DoDI 2000.12, "DoD Antiterrorism Program," September 9, 2013
   vi. DoDI 2000.16, "DoD Antiterrorism Standards," December 8, 2006
   vii. DoDI 5200.08-R, "Physical Security Program," April 9, 2007
   viii. DoDI 5200.08, "Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)," December 10, 2005
   ix. DoDD 3000.3, "Policy for Non-Lethal Weapons," July 9, 1996
   x. Unified Facilities Criteria 4-010-01, "DoD Minimum Antiterrorism Standards for Buildings," February 9, 2012

xi. FIPS 201, "Federal Information Processing Standards Publication Personal Identity Verification of Federal Employees and Contractors," June 23, 2006

xii. 10 U.S.C. Subtitle C, Authority, Law Enforcement, Security of Naval Installations, Security of DoD Installations

b. U.S. Navy policy and guidance directives:

i. SECNAV M-5510.30, "DoN Personnel Security Program," June 2006

ii. SECNAV M-5510.36, "DoN Information Security Program," June 2006

iii. SECNAVINST 5510.37 "DoN Insider Threat Program," August 8, 2013

iv. SECNAV Directed Installation Security Posture Assessment, September 17, 2013

v. CNO Antiterrorism Strategic Guidance 2010, September 2010

vi. OPNAVINST 3400.12, "Navy Required Operational Capability Levels for Navy Installations and Activities," October 6, 2008

vii. OPNAVINST 3300.53C, "Navy Antiterrorism Program," May 26, 2009

viii. OPNAVINST 5530.14E, "Navy Physical Security and Law Enforcement Program," January 28, 2009

ix. OPNAVINST 3591.1F, "Small Arms Training and Qualification," August 12, 2009

x. Navy-wide OPTASK Antiterrorism, March 18, 2013

xi. U.S. Fleet Forces, Antiterrorism Operations Order 3300-13, January 2013

xii. U.S. Pacific Fleet, Operations Order 201, September 2007

xiii. U.S. Naval Forces Southern Command, Operations Order 4000-07, October 2007

xiv. U.S. Naval Forces Europe, Operations Order 4000-05 April 2006

xv. U.S. Naval Forces Central Command, Operations Order 09-1, December 2009

c. Geographic Combatant Commander policy and guidance directives:

i. USNORTHCOM Antiterrorism Instruction 10-222

ii. USEUCOM Antiterrorism Operations Order 11-05

iii. USCENTCOM Antiterrorism Operations Order 05-02

iv. USPACOM Antiterrorism/CIP Operations Order 5050-08

v. USSOUTHCOM SC Regulation 380.16

vi. USAFRICOM AT-CIP Operations Order 10-06

3. Definitions and Terms of Reference

a. Access Control. An integral and interoperable part of Department of Defense installation physical security programs. Each installation commander and facility director must clearly define, consistent with Department of Defense policy, the access control measures (tailored to local conditions) required to safeguard personnel, facilities, protect capabilities and accomplish the mission.

b. Force Protection. Preventive measures taken to mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities and critical information. Force protection does not include actions to defeat the enemy or protect against accidents, weather or disease.

c. Insider Threat. A person with authorized access, who uses that access, wittingly or unwittingly, to harm national security interests or national security through unauthorized disclosure, data modification, espionage, terrorism or kinetic actions resulting in loss or degradation of resources or capabilities. The term kinetic can include, but is not limited to, the threat of harm from sabotage or workplace violence.

d. Physical Security. That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material and documents; and to safeguard them against espionage, sabotage, damage and theft.

e. Risk. Probability and severity of loss linked to hazards.

f. Tactical Control. Command authority over assigned or attached forces or commands, or military capability or forces made available for tasking, that is limited to the detailed and, usually, local direction and control of movements or maneuvers necessary to accomplish missions or tasks assigned. Tactical control is inherent in operational control. Tactical control may be delegated to, and exercised at any level at or below the level of combatant command.

g. Tactical Control for Force Protection. Tactical Control that enables the Geographic Combatant Commander to order implementation of force protection measures and to exercise the security responsibilities outlined in any memorandum of agreement concluded pursuant to memorandum of understanding between the Department of State and the Department of Defense, "Security of DoD Elements and Personnel in Foreign Areas," December 16, 1997 (known as the "Universal Memorandum of Understanding"). Further, Tactical Control for Force Protection authorizes the Geographic Combatant Commander to change, modify, prescribe and enforce force protection measures for covered forces. This relationship includes the authority to inspect and assess security requirements, and submit budget requests to parent organizations to fund identified corrections. The Geographic Combatant Commander may also direct immediate Force Protection Condition measures (including temporary relocation and departure) when in his judgment such measures must be accomplished without delay to ensure the safety of Department of Defense personnel involved. Persons subject to Tactical Control for Force Protection of a Geographic Combatant Commander include Active and Reserve Component personnel (including National Guard personnel in a title 10 status) in the Area of Responsibility.

4. Force Protection

a. Theory:

i. The Geographic Combatant Commander exercises Tactical Control for Force Protection of all Department of Defense forces in the commander's Area of Responsibility and stipulates how the Tactical Control for Force Protection of Navy forces is delegated. The delegation of Tactical Control for Force Protection is most commonly implemented along Service or functional component lines or geographically determined sectors. Once designated by the Geographic Combatant Commander, Navy Fleet Commanders further define the Tactical Control for Force Protection chain of command for Navy forces, to include Navy installations and tenants located within each Area of Responsibility. Each Fleet Commander promulgates this Tactical Control for Force Protection chain of command by Operations Order or instruction.

ii. Services and Geographic Combatant Commanders provide broad physical security policy which commanders use to tailor their own specific guidance and directives. Using this guidance and the results of prior risk assessments, commanders promulgate physical security guidance and directives to set an appropriate force protection posture. Commanders ensure continued compliance with and execution of all physical security guidance and directives through higher headquarters assessments and periodic observation of exercises.

iii. Navy force protection is aligned with higher headquarters directives and is intended to mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities and critical information. Physical security, as a sub-set of force protection, is concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material and documents; and to safeguard them against espionage, sabotage, damage and theft.

iv. The Navy implements physical security through the defense-in-depth model based on the Department of Defense Antiterrorism Standard 13 (detect, assess, communicate, delay, deny and respond). This model employs six key elements: access control, pier security, waterside security, response capability, High Value Unit transit escort and Random Antiterrorism Measures.

v. By design, this model is intended to protect Navy assets and personnel from external threats through prevention of unauthorized access to our installations, either through denial of access or the use of lethal force. Inherent in the Navy's physical security model is the assumption that established vetting and credentialing processes ensure that those who have been properly vetted and credentialed remain loyal, trustworthy, and reliable--thereby mitigating the potential for insider attack. Additionally, Navy physical security addresses the insider threat through the use of Random Antiterrorism Measures and a rapid, robust response capability to discourage the would-be insider.

vi. The Navy uses a risk-based security strategy to prioritize and employ Navy security forces and capabilities in accordance with the Chief of Naval Operations' installation Required Operational Capabilities tiering system. The Required Operational Capabilities tiering system prioritizes installation physical security requirements according to the installation's operational missions and tenant and installation criticality. To support Required Operational Capabilities tiering system manning requirements, the Navy has implemented the Mission Profile Validation-Protection manpower model, which identifies the minimum manning required to set desired protection capabilities at each Navy installation--this model identifies the minimum manning required to implement installation physical security requirements up to Force Protection Condition Bravo. To support physical security manpower requirements beyond Force Protection Condition Bravo, the Navy uses an Auxiliary Security Force model, which requires installation tenants and berthed ships to augment installation security forces with personnel trained to execute force protection watchstanding requirements.

b. Assumptions (Assumption. *Basis--drawn from a compilation of the references noted in paragraph 2*):

i. Department of Defense vetting and credentialing procedures are effective. *Department of Defense policy*

ii. Everything cannot be protected against every threat. *Navy risk-tiered security strategy*

iii. Random Antiterrorism Measures are an effective deterrence and interrupt terrorist operational planning. *Navy policy*

iv. The conduct of 100 percent vehicle, personnel and baggage checks in Force Protection Condition Alpha is not required (lack of specific, credible threat reporting). *Navy policy*

v. Department of Defense credentialing programs enable use of a trusted traveler policy in Force Protection Condition Alpha as authorized by DTM 09-12. *Department of Defense policy*

vi. The intelligence communities' threat analyses are accurate. *Navy policy*

vii. Based upon the intelligence community's assessment, the threat to Navy forces in the Continental United States is low. *U.S. Fleet Forces assessment analysis*

viii. Existing installation Mutual Support Agreements with off-base agencies are executable. *Navy policy*

ix. Current Navy force protection training is sufficient and focused on the correct threats. *Navy policy*

x. Installation and external agency response forces will rapidly mitigate and neutralize a potential threat. *Navy policy*

5. Assessment

a. Risk Assessment. An assessment of risk to Navy forces is comprised of an examination of three primary elements: criticality, threat and vulnerability (risk = criticality x threat x vulnerability). In order to set an appropriate force protection posture, all Fleet Commanders periodically conduct risk assessments. The elements of a risk assessment will vary according to the specific threats within the Area of Responsibility and Geographic Combatant Commander guidance. For bases, stations and installations in the continental United States, U. S. Fleet Forces used the results of the recently completed Force Protection Baseline Review which included a detailed risk assessment for Navy forces located in the U.S. Northern Command Area of Responsibility (Tab A refers). This assessment prioritized all Navy assets in to broad categories of high, medium and low based upon criticality to operational missions. Naval Criminal Investigative Service Multiple Threat Alert Center, in conjunction with the wider intelligence community, determined the most likely and most dangerous threats to Navy assets and personnel in the U. S. Northern Command Area of

Responsibility. Naval Criminal Investigative Service assessment subject matter experts then conducted focused vulnerability assessments of Navy assets and personnel, against the identified most likely and most dangerous threats. For bases, stations and installations outside the United States, Fleet Commanders leveraged their latest risk assessment and continuous assessment process data.

b. Adequacy of Navy physical security guidance and directives. Fleet Commander subject matter experts examined Navy physical security directives and guidance to ensure that current policy requirements establish a defense-in-depth through the employment of the detect, assess, communicate, delay, deny and respond construct (Department of Defense Antiterrorism Standard 13). This review verified that current policy requirements are adequate to enable the setting of an effective force protection posture.

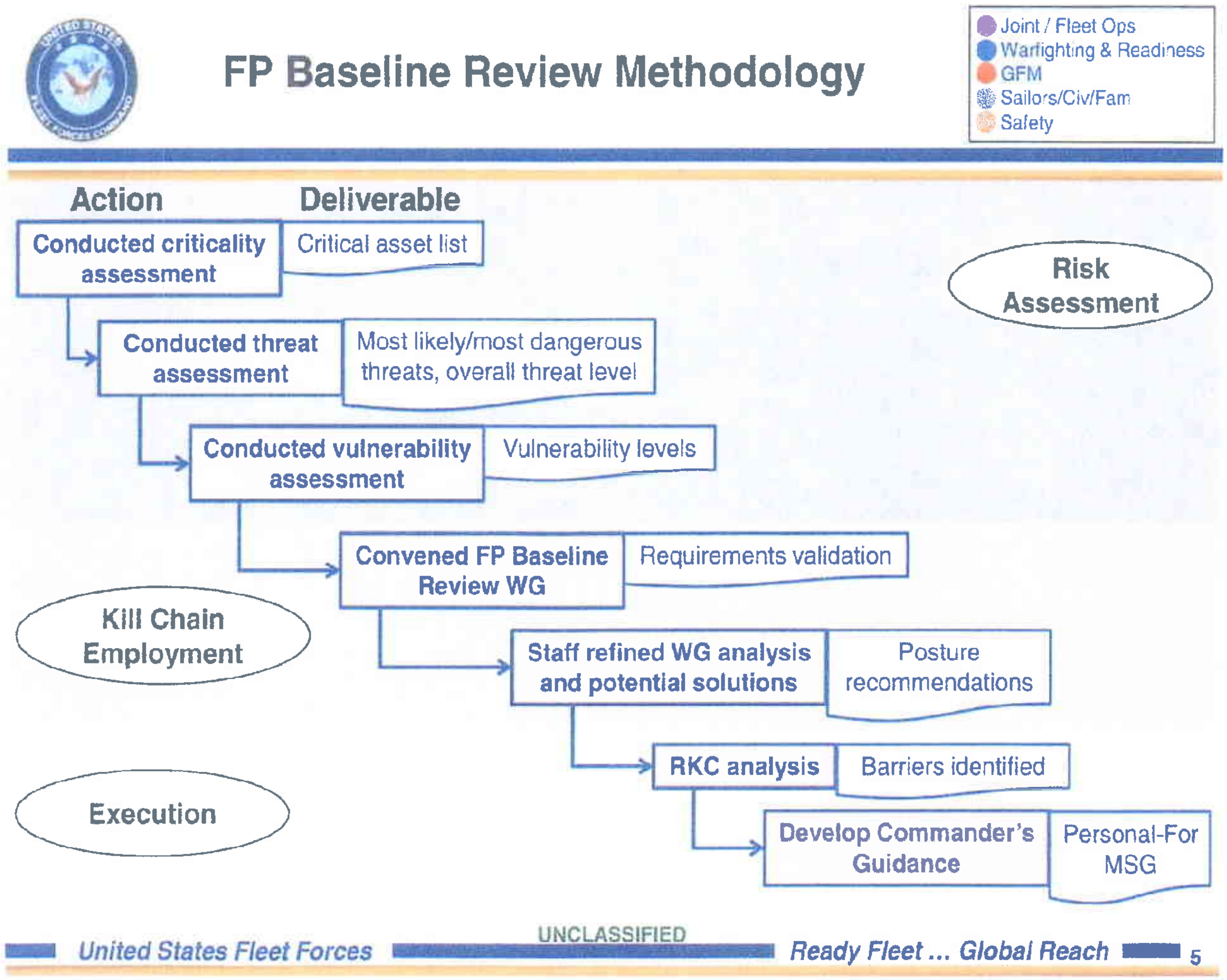
c. Alignment with physical security guidance and directives. Prior to issuance of their own guidance, Fleet Commanders ensure alignment with Navy and Geographic Combatant Commander physical security guidance and directives. During this assessment, all Fleet Commander physical security directives were examined and found to be in alignment with Department of Defense, Secretary of the Navy, Chief of Naval Operations and Geographic Combatant Commander guidance.

d. Compliance with physical security guidance and directives. Fleet Commanders ensure compliance with all physical security guidance and directives through periodic observation of exercises and higher headquarters assessments. For this assessment, the Fleet Commanders reviewed the results of recent annual antiterrorism exercises along with data from tailored higher headquarters assessments to determine whether Navy security forces remain compliant with all physical security guidance and directives. This review concluded that Navy security forces are in compliance with physical security guidance and directives.

e. Assessment of security and force protection policy execution at tactical level. Fleet and Region Commanders assess execution of physical security and force protection policy through assessments and exercise evaluations. Fleet and Navy Region Commanders regularly assess installation security forces' ability to execute security and force protection policy at the tactical level via the U. S. Fleet Forces higher headquarters operational assessments at installations inside the continental United States--and using Installation Protection Cell assessments at installations outside the continental United States. Additionally, annual antiterrorism exercises, such as Citadel Pacific, Reliant Defender and Solid Curtain-Citadel Shield, provide opportunities to improve tactical execution by evaluating unit and installation performance using the parameters of the Navy Security Operations Exercise Program. The review of the results of these periodic assessments and antiterrorism exercises indicate Navy security forces are properly executing security and force protection policy at the tactical level.

f. Adequacy of response forces and Mutual Support Agreements. A review by Fleet and Navy Region Commanders concluded that Navy installation physical security programs possess adequate response force capability either via organic security forces, as augmented by Auxiliary Security Forces, or through comprehensive Mutual Support Agreements with local, state and federal agencies; and Status of Forces Agreements with host nations.

TAB A



FP Baseline Review Methodology

● Joint / Fleet Ops
● Warfighting & Readiness
● GFM
● Sailors/Civ/Fam
● Safety

Action	Deliverable
Conducted criticality assessment	Critical asset list
Conducted threat assessment	Most likely/most dangerous threats, overall threat level
Conducted vulnerability assessment	Vulnerability levels
Convened FP Baseline Review WG	Requirements validation
Staff refined WG analysis and potential solutions	Posture recommendations
RKC analysis	Barriers identified
Develop Commander's Guidance	Personal-For MSG

Risk Assessment

Kill Chain Employment

Execution

United States Fleet Forces UNCLASSIFIED Ready Fleet ... Global Reach 5

Marine Base, Station and Installation Physical Security Assessment Report

September 27, 2013

Encl (2)

Scope: This report provides a "quick look" world-wide assessment of current physical security and access control measures at Marine Corps owned and operated installations, as directed by the Chief of Naval Operations (CNO) and Commandant of the Marine Corps (CMC) in a joint letter dated 23 September 2013. This assessment addresses adequacy of Marine Corps physical security directives and policies as well as compliance with those governing directives and policies. A more in-depth review will be completed no later than 31 October 2013.

Methodology: Commander, Marine Corps Forces Command (COMMARFORCOM) led an Operational Planning Team (OPT) to review the adequacy of Marine Corps physical security policies and directives. OPT members included Deputy Commandant, Plans, Policy and Operations (DC PP&O) Security Division (PS), Marine Corps Installations Command (MCICOM), Training and Education Command (TECOM), Marine Corps Recruiting Command (MCRC) and Marine Forces Reserve representatives. OPT members reviewed policies referenced in Tab A. Marine Corps policies and directives were reviewed to ensure consistency with DoD and DoN guidance and compliance with objectives laid out in the 2012 DoD Mission Assurance Strategy. The OPT also considered potential gaps in Marine Corps directives and policies relative to DoD/DoN/Service policies, emerging threats or other areas.

In addition to the policy review, this Marine Corps assessment considered screening and vetting of personnel, access control, security programs and systems, insider threat awareness, training, and execution of Force Protection. The Marine Corps based its assessment on:

- A review of DoD, DoN, and Marine Corps mission assurance, physical security, anti-terrorism and other force protection policies and directives. (A complete list of documents reviewed is included in Tab A).
- An electronic survey provided to commanders at 24 Marine Corps installations world-wide.
- Direct discussions with Installation Commanders and Commanding Generals, Marine Corps Installations Command (MCICOM), Training and Education Command (TECOM), Marine Corps Recruiting Command, (MCRC), Marine Forces Reserve (MFR), Marine Corps Installations East, Marine Corps Installations National Capital Region, Marine Corps Installations West and Marine Corps Installations Pacific.
- A review of all Mission Assurance Assessment Team (MAAT) and Inspector General reports conducted over the past three years.

Quick Look Assessment: The Marine Corps Mission Assurance framework (to include physical security and access control) and supporting processes protect the force (to include our civilian Marines and our family members aboard Marine Corps Installations), systematically assess and manage enterprise risk, synchronize protection-related programs and activities, and prioritize investments to ensure mission performance given available resources. Marine Corps physical security policy is adequate and aligned with higher authorities. However, there are known discrepancies or gaps in execution that are being mitigated or are under review.

- Marine Corps physical security and access control policies and regulations provide adequate direction to protect the force against anticipated threats.
- The Marine Corps is partially compliant in executing physical security and access control directives as part of a broader, integrated Mission Assurance (MA) process that includes risk mitigation measures.
- Installation commander programs are dependent upon coordinated efforts of Marine Corps and other Service and Agency tenant organizations. These relationships should be more clearly defined and codified in policy.

- Limited resources (personnel, equipment, funding) coupled with varying base specific/unique characteristics create shortfalls in compliance and gaps in protection. These discrepancies are identified and prioritized for mitigation.

Physical Security and Access Control Policy. Service-level policies and regulations regarding physical security and access control are in alignment with applicable DoD and DoN directives and instructions. Marine Corps physical security and access control policies and regulations can be attributed directly to requirements stipulated in DoD and DoN policies. These policies provide procedures, standards, planning guidance, associated details, and requirements to support protection programs at all echelons of command. Additionally, the Marine Corps approach to physical security and access control is in alignment with the DoD Mission Assurance Strategy.

The Marine Corps complies with DoD/DoN/Service policies by:

- Developing and implementing policies to secure forces, facilities and infrastructure against anticipated threats (enemy activity, terrorism, crime, insider threats, natural disasters, accidents and health threats).
- Identifying a dedicated Service Protection Advocate (DC PP&O) to coordinate and synchronize common, overlapping, and unique requirements of protection programs Marine Corps-wide; advising the Commandant on priorities for management of risks across various programs and activities.
- Implementing routine, streamlined, and standardized Mission Assurance Assessment (MAA) Program methodology to evaluate installations world-wide on a triennial basis. The MAA is a consolidated assessment and inspection program that integrates all aspects of Mission Assurance (to include physical security and access control). It provides commanders with informed results to support risk management. MAAs are led by DC PP&O (PS) and conducted at all Marine Corps installations. Since implementation of the MAA program in July 2010, all 24 Marine Corps installations were assessed at least once. Results of MAAs are used to assist installations to identify vulnerabilities, comply with broader DoD Mission Assurance policies and to ensure effective identification, assessment, and mitigation of risk to installations and tenant organizations.
- Utilizing both formal (i.e. DoD and Service working groups) and informal mechanisms to continually refine Service policies and ensure alignment with new strategies, requirements and threats.

Screening/Vetting of Personnel. Requirements for vetting and screening personnel who access Marine Corps installations are established by policy, orders, and directives, but are not universally followed as required.

A National Agency Check and Law and Credit Check (NACLC) is required to establish enlistment and appointment suitability. This program helps discover if prospective Service members are the subject of felony warrants, have connections to foreign intelligence services, are members of radical organizations, or have documented significant mental health issues which may impact reliability. A satisfactory result from a NACLC serves as the basis for issuance of the Common Access Card (CAC) and eligibility for a Secret level security clearance. The investigation is initially prepared and submitted by recruiters. In limited circumstances, a new Marine may be issued a CAC prior to completion of the investigation, but still will not have been granted eligibility for a SECRET clearance. This occurs at a rate of approximately 12% of the Marine Corps' annual accessions. Marine Corps commands are working to complete open investigations for Marines.

Civilian employees undergo the National Agency Check with Written Inquiries (NACI) to establish government employment suitability and when suitable, the issuing of CACs. The NACI is also the minimum investigation required for issuance of the CAC for contractors. A policy revision in 2012 relieved the Department of the Navy Central Adjudication Facility (DONCAF) of NACI adjudication responsibilities. Initiating commands are currently responsible for decisions about retention and CAC issuance. This change decentralized oversight and reduced DoN CAC issuance standardization.

Personnel Security Programs include a Continuous Evaluation Program (CEP) component, which requires commanders to report derogatory information (e.g. misconduct, credit issues, etc...) concerning individuals possessing security clearance eligibility. A gap has been identified in CEP execution, as not all derogatory information is properly reported to DONCAF. Commanders' CEP reporting may result in uneven application of program standards in adjudication of new information.

Access control. DoD and DoN policy require, at a minimum, a physical and visual inspection of all approved identification badges, including a visual match of the badge's photograph to the person presenting the card. Gate sentries are required to conduct a hands-on physical inspection of every ID card presented; however, rush hour traffic issues significantly impact access routes on and off installations and, therefore, preclude adherence to policy requirements during those hours. Survey feedback suggests safety concerns related to traffic congestion, efforts to be good neighbors with surrounding communities, and sheer traffic volume cause installation commanders to accept risk.

Access control requires sufficient numbers of trained installation law enforcement/security personnel employed effectively and utilizing appropriate equipment and technology (such as readily accessible National Crime Information Center computer terminals) combined with appropriate facilities and infrastructure to provide a layered "defense-in-depth." Survey feedback identifies manning and technology shortfalls as the direct cause of gate closures, restricted access and reduced hours of operation.

Security Programs and Systems. Marine Corps security programs and systems cover a range of activities including; security and law enforcement (LE), antiterrorism, physical security and electronic security systems, emergency management, critical infrastructure protection, chemical, biological, radiological and nuclear protection. Resourcing challenges are common across these programs.

The Marine Corps security services requirement defines the number of armed personnel required to support security and law enforcement aboard installations. The current requirement consists of a mix of Military Police, civilian police and Fleet Assistance Program (FAP) personnel. Civilian police are recruited, trained, and managed under the Marine Corps Civilian Law Enforcement Program (MCCLEP). FAP personnel are provided by tenant commands, usually for periods of 6 months or less. The total armed requirement is approximately 3,000 (1,400 MPs 1,147 civilian police, and 433 FAPs). There are also approximately 600 support personnel providing 911 emergency dispatch, alarm monitoring, physical security, and contractor and visitor vetting service, among other security and LE support functions. MCCLEP is currently not fully resourced and is being assessed for remediation.

This quick look indicated that, although not a current organic installation requirement, Special Reaction Teams provide an important security capability. Many installations have agreements with tenant commands to provide Security Augmentation Forces (SAF) to the installation to support policing and security activities during high threat periods.

Insider Threat Awareness. In 2010, the Marine Corps established the Marine Corps Insider Threat Working Group. It provides service level awareness and support to DoN Program development. SECNAVINSTR 5510.37 sets forth amplifying department level direction for insider threat program and is currently being implemented across the Marine Corps. The Marine Corps recently established the Violence Prevention Program (VPP). VPP works in conjunction with other programs to assess, mitigate, and respond to acts or threats of violence or other inappropriate behavior. All threats are taken seriously and installation Provost Marshal Offices /Human Resource Offices are notified as protocol. Recognizing warning signs of potential violence is the foundation of this program and is the responsibility of all personnel. Refresher training for Violence Prevention Officers (VPOs) is required to enable the recognition of specific components of intended violent acts, including means, opportunity, and motivation to carry out a threat that may indicate imminent violence. This program is not currently applicable to civilian or contractor personnel.

Privately owned weapons aboard installations raise potential insider threat considerations. Service and DoD level personal weapons policy provides commanders various authorities to establish guidance for storage of personal arms and ammunition. Installation polices are not consistently followed. Although not directed, commanders may conduct regular checks for personally owned weapons via RAM, barracks inspections and vehicle inspections aboard installations. Incident Complaint Reports related to personal weapons are collected and tracked by the Service and the Naval Criminal Investigative Service and reported annually.

Training. Compliance with force protection training requirements varies based on whether the training audience is military, civilian, contractor or family members. Based on survey responses, the Marine Corps could improve violence prevention/threat response training for tenant commands. Most Marine Corps installations have active shooter-specific incident response plans and can notify military personnel to shelter in place (SIP) or evacuate through mass notification systems. Evacuation training or SIP specific to active shooter events is not provided to civilian/contractor personnel.

Execution of Force Protection. Installation commanders' authority for security program management is derived from both DoD, DoN and Marine Corps level guidance. Tenant commanders follow and support installation commander security guidance. However, installation commanders have no means to track and ensure compliance. Installation commander programs are dependent upon coordinated efforts with their tenant commands across all assessed areas. This includes compliance reporting, resource sharing to mitigate shortfalls, and monitoring of personnel as in the Continuous Evaluation Program. The relationship between Installation Commander and tenant commands is central to success. These relationships should be clearly defined and codified in policy.

Installation commanders' efforts to mitigate adverse impacts from man-made and natural threats are bound by installation configuration (open vs. closed bases), proximity to surrounding civilian communities/populations, tenant/base relationships and operating policies, as well as geophysical constraints. Commanders' ability to fully comply with DoD, DoN and Service physical security and access control policies is effected by each installation's available resources and unique set of geophysical characteristics (i.e. a Marine Corps installation such as Quantico with a town in the middle of the base).

Areas for further study: Further analysis of installation security beyond this quick look is required to identify recommendations and actions based on emerging threats and the fiscal landscape. Topics for further study include:

- Review Marine Corps vetting and credentialing procedures.
- Review Service access control policy and procedures.
- Review funding profiles and requirements for security encompassing infrastructure enhancement, access control, law enforcement, military police and information/personnel security manpower requirements for resourcing within the budget process.
- Review installation command and tenant commander/activity relationships.
- Evaluate technology enhancement options to mitigate risk and offset resource shortfalls.
- Examine training and education programs to identify contributing factors and behavioral indicators of potentially violent actors and to increase commander awareness of the need for continuous evaluation.
- Review personal weapons policies and procedures for uniformity and enforcement.

TAB A
POLICY REFERENCES

1. Executive Order (EO) 10450, Security Requirements For Government Employment, as amended
2. EO 12968, Access To Classified Information And Background Investigations Standards, as amended
3. EO 13467, Reforming Processes Related To Suitability For Government Employment, Fitness For Contractor Employees, And Eligibility For Access To Classified National Security Information
4. EO 13587, Structural Reforms To Improve The Security Of Classified Networks And The Responsible Sharing And Safeguarding Of Classified Information
5. EO 13488, GRANTING RECIPROCITY ON EXCEPTED SERVICE AND FEDERAL CONTRACTOR EMPLOYEE FITNESS AND REINVESTIGATING INDIVIDUALS IN POSITIONS OF PUBLIC TRUST
6. 10 U.S.C. SUBTITLE C, Authority, Law Enforcement, Security Of Naval Installations, Security Of DoD Installations
7. FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION (FIPS) 201, Personal Identity Verification (OIV) Of Federal Employees And Contractors - 23 JUN 2006
8. UNIFIED FACILITIES CRITERIA (UFC) 4-010-01, with change 1, DoD Minimum At Standards For Buildings – 9 FEB 2012
9. UFC 4-022-01 - 25 MAY 2005: Security Engineering: Entry Control Facilities/Access Control Points
10. UFC 4-021-01, with change 1, Design And Operations Management: Mass Notification Systems - JAN 2010
11. Homeland Security Presidential Directive (HSPD) 12, Policies For A Common Identification Standard For Federal Employees And Contractors - 27 AUG 2004
12. OSD 07688-10-1, Final Recommendations Of The Fort Hood Follow On Review
13. DOD 5200-08-R with change 1: Physical Security Program - 1 MAY 2009
14. DODI 2000.12, DoD Antiterrorism Program - 09 SEP 2013
15. DODI 2000.16, DoD Antiterrorism Standards - 08 DEC 2006
16. DODI 2000.26, Suspicious Activity Reporting – 1 NOV 2011
17. DODI 5200.08 with change 1, Physical Security Of DoD Installations And Resources And The DoD Physical Security Review Board (PSRB) - 10 DEC 2005
18. DODI 6055.17, Installation Emergency Management Program - 13 JAN 2009
19. DIRECTIVE TYPE MEMORANDUM (DTM) 09-12 with change 3: Interim Policy Guidance For DoD Physical Access Control - 8 DEC 2009
20. SECNAVINST 5510.30B & SECNAV M5510.30, DoN Personnel Security Program – 6 OCT 2006
21. SECNAVINST 5510.36A & SECNAV M5510.36, DoN Information Security Program – 6 OCT 2006
22. SECNAVINST 5510.37, DoN Insider Threat Program – 8 AUG 2013
23. NAVMC 3500.103: Navy Marine Corps Anti-Terrorism Manual - 27 OCT 2010
24. Naval Message 232055Z JUL 10, SUBJECT: Interim USMC Role Player Threat And Screening Program Policy
25. MCO 3302.1E, Marine Corps Antiterrorism Program - 08 MAR 2009
26. MCO 3440.9, Marine Corps Installation Emergency Management Program - 1 SEP 2010
27. MCO 5510.18A, with change 2, Marine Corps Information And Personnel Security Program – 25 JUN 2002
28. MCO 5530.14A, Marine Corps Physical Security Program Manual - 05 JUN 2009
29. MCO 5530.16, Security Augmentation Force Program – 26 AUG 2011
30. MCO P5580.2B with change 1, The USMC Law Enforcement Manual - 27 DEC 2011
31. MCO P11000.11, Marine Corps Fire Protection And Emergency Services Program – 23 JUN 2010
32. MARADMIN 533/08, Installation Access Control Policy
33. MARADMIN 098/10, HSPD 12 Compliance Within The Marine Corps